947

Monge, Elaine (SCA)

From: jason.bernstein@btlaw.com <noreply+76d1e4b69cb4a307@formstack.com>
Sent: Wednesday, July 13, 2016 11:54 AM
To: Breaches, Data (SCA)
Subject: Security Breach Notifications

Formstack Submission for form Security Breach Notifications

Submitted at 07/13/16 11:53 AM

Business Name:	Outten & Golden LLP
Business Address:	3 Park Avenue 29th Floor New York, NY 10016
Company Type:	Commercial
Your Name:	Jason Bernstein
Title:	Partner
Contact Address:	3475 Piedmont Road, NE Suite 1700 Atlanta, GA 30022-3327
Telephone Number:	(404) 264-4040
Extension:	
Email Address:	jason.bernstein@btlaw.com
Relationship to Org:	Third party provider
Breach Type:	Electronic
Date Breach was Discovered:	06/18/2016
Number of Massachusetts Residents Affected:	1
Person responsible for data breach.:	Current Employee
Please give a detailed explanation of how the data breach occurred.:	Employee was a victim of a phishing attack and sent a file with the W2 information of the firm's employees to an unauthorized email address.
Please select the type of personal information that was included in the breached data.:	Social Security Numbers = Selection(s)
Please check ALL of the boxes that apply to your breach.:	The breach was a result of a malicious/criminal act. = Selection(s)

For breaches involving paper: A lock or security mechanism was used to physically protect the data.:	N/A
Physical access to systems containing personal information was restricted to authorized personnel only.:	N/A
Network configuration of breached system:	Internet Access Available
For breaches involving electronic systems, complete the following:	Personal information stored on the breached system was password-protected and/or restricted by user permissions. = Selection(s)
All Massachusetts residents affected by the breach have been notified of the breach.:	Yes
Method(s) used to notify Massachusetts residents affected by the breach (check all that apply)::	E-mail = Selection(s)
Date notices were first sent to Massachusetts residents (MM/DD/YYYY):	06/19/2016
All Massachusetts residents affected by the breach have offered complimentary credit monitoring services .:	Yes
Law enforcement has been notified of this data breach.:	Yes
Please describe how your company responded to the breach. Include what changes were made or may be made to prevent another similar breach from occurring.:	The company investigated the breach to determine the cause. Improved procedures were implemented for verifying/validating information requests (e.g., W-2 requests).

Monge, Elaine (SCA)

From: Bernstein, Jason <Jason.Bernstein@btlaw.com>
Sent: Wednesday, July 13, 2016 11:59 AM
To: Breaches, Data (SCA)
Subject: Notification of data breach
Attachments: Outten & Golden-L-Breach Notification to Authorities - VA.pdf; O&G-Data Security Incident Notification Form - MA.pdf; O&G-Security Breach Notifications Submission (Consumer Affairs)-MA.PDF

Greetings:

As required, please see the attached letter being sent today to the Mass. Attorney General's office. Notice was also submitted today to the Consumer Affairs and Business Regulation office via the online form.

Please let me know if you need additional information.

Jason A. Bernstein

BARNES & THORNBURG LLP

VCard | Bio | Dept Info

Jason A. Bernstein
Phone: (404) 264-4040
Fax: (404) 264-4033
jason.bernstein@btlaw.com

Partner, Intellectual Property Group
- Data Security & Privacy (co-chair)
- Technology Agreements
- Patent, Trademark, Copyright Law

Barnes & Thornburg LLP
Prominence In Buckhead
3475 Piedmont Road, N.E.
Suite 1700
Atlanta, Georgia 30305-3327
www.btlaw.com

ATLANTA CHICAGO DALLAS DELAWARE INDIANA
LOS ANGELES MICHIGAN MINNEAPOLIS OHIO WASHINGTON, D.C.

Young folks know the rules; old, the exceptions (O.W. Holmes)

BARNES & THORNBURG LLP

Prominence in Buckhead
3475 Piedmont Road, N.E., Suite 1700
Atlanta, Georgia 30305-3327
404-846-1693 (Main)
404-264-4033 (Fax)
www.btlaw.com

Jason A. Bernstein
404-264-4040 (Direct Dial)
jason.bernstein@btlaw.com

July 12, 2016

Computer Crime Section
Virginia Attorney General's Office
202 North 9th Street
Richmond, VA 23219

Re: Reporting Data Security Incident

Greetings:

On behalf of Outten & Golden LLP we submit herewith the enclosed data security incident notification information, as required under Virginia.

If you require any additional information, please contact me.

Sincerely,

Jason A. Bernstein
Barnes & Thornburg LLP

JAB/c
Enclosure
cc: Victoria Spencer Patterson (w/ enclosure, via email)
4098360_1.docx

MASSACHUSETTS STATE SECURITY INCIDENT REPORT

Name and address of Entity that owns or licenses the computerized data that was subject to the breach:
Outten & Golden LLP
Street Address: 3 Park Avenue, 29th Floor
City: New York State: NY Zip Code: 10016

Submitted by: Jason A. Bernstein Title: Attorney Dated: July 13, 2016
Firm Name (if other than entity): Barnes & Thornburg LLP
Telephone: 404-264-4040 Email: jason.bernstein@btlaw.com
Relationship to Entity whose information was compromised: Attorney for Outten & Golden LLP

Type of Organization (please select one): [ ] Governmental Entity; [ ] Other Governmental Entity;
[ ] Educational; [ ]Health Care; [ ]Financial Services; [X]Other Commercial; or [ ]Not-for-profit.

Number of Persons Affected:
Total: 157 Massachusetts Residents: 1

Dates: Breach Occurred: June 18, 2016 Breach Discovered: June 18, 2016 Affected Individuals Notified: June 19, 2016

Description of Breach (please select all that apply):
[ ]Loss or theft of device or media (e.g., computer, laptop, external hard drive, thumb drive, CD, tape);
[ ]Internal system breach; [ ]Insider wrongdoing; [ ]External system breach (e.g., hacking);
[X]Inadvertent disclosure ; [X]Other specify): Employee was a victim of a phishing attack and sent a file with the W2 information of the firm's employees to an unauthorized email address

Information Acquired: Name or other personal identifier in combination with (please select all that apply):
[X]Social Security Number
[ ]Driver's license number or non-driver identification card number
[ ]Financial account number or credit or debit card number, in combination with the security code, access code, password, or PIN for the account

Manner of Notification to Affected Persons - ATTACH A COPY OF THE TEMPLATE OF THE NOTICE TO AFFECTED RESIDENTS:
[X] Written [X] Electronic [ ] Telephone [ ] Substitute notice
List dates of any previous (within 12 months) breach notifications: _____

Identify Theft Protection Service Offered: [X]Yes [ ] No
Duration: 12 months Provider: AllClearID
Brief Description of Service: Credit monitoring; the firm is also reimbursing employees for the cost of freezing credit.

TEMPLATE OF COMMUNICATION SENT TO AFFECTED INDIVIDUALS

Dear [redacted],

We value and respect the privacy of your personal information. Therefore, we are writing to inform you of an incident involving some of that information, what that means to you, how we are actively addressing the situation, and what you might do to protect yourself.

The Facts As We Currently Know Them

Late Friday afternoon, June 17, 2016, the firm learned that, as a result of a spoofing attack, your W2-related information has been compromised and accessed by unauthorized persons. As soon as we became aware of the incident, we started addressing the situation.

First, we sent an email late Friday afternoon to [redacted] about the episode. Subsequently, we retained counsel who are experienced in dealing with such situations. The incident and pertinent details are being reported to the appropriate agencies, and we are fully cooperating with them. We are sending this information via email today; we will be sending it again via mail on Monday.

We believe that fewer than 200 current and former employees may have been affected. While we are unable to determine exactly the extent to which the information has been accessed and/or used, we have received at least one report of an employee's information being used improperly.

What Type of Information Was Involved?

The information that may have been accessed included identifying personal information, such as name, address, and social security number.

Steps You Should Take to Protect Yourself

Because the firm takes the protection of your personal security very seriously, we are offering free credit monitoring services. We are contracting with a credit monitoring service to offer you 12 months of services at no cost to you. This product helps detect possible misuse of your personal information and provides you with identity protection support focused on immediate identification and resolution of identity theft. We will provide a follow up letter shortly that will include instructions for contacting the service provider. Lastly, see the enclosed information for additional steps you should take to protect yourself.

Contact Information

If you have any questions, please contact:

Victoria Spencer Patterson, Director of Administration
Outten & Golden LLP
3 Park Ave, 29th Floor, New York, NY 10016
Phone: 646-825-9807
Fax: 646-509-2082
Email: vsp@outtengolden.com

We apologize for any inconvenience this may have caused. Be assured that we have been working, and will continue working, diligently to avoid and mitigate any harm to you.

Sincerely,

Wayne N. Outten
Managing Partner

STEPS YOU CAN TAKE TO FURTHER PROTECT YOURSELF

We are providing this explanation of steps you can take to protect your information. As a precautionary measure, we recommend that you remain vigilant for incidents of fraud and identity theft by reviewing your account statements and credit reports closely. You may obtain a free copy of your credit report from each of the three major credit reporting agencies listed below once every 12 months by visiting http://www.annualcreditreport.com or calling toll-free 877-322-8228. You can also report any fraudulent activity or any suspected identity theft to proper law enforcement authorities, your state attorney general and/or the Federal Trade Commission. To file a complaint about identity theft with the FTC or to learn more, go to www.ftc.gov/idtheft, call 1-877-ID-THEFT (877-438-4338).

Fraud Alert

We suggest you consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. If you would like to place a fraud alert on your credit report, contact any of the three credit reporting agencies using the contact information below. The Federal Trade Commission has a good website with an overview and guidance on this issue at https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs. You can also contact them at: Federal Trade Commission or write to: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Or, call 1-877-ID-THEFT.

Security Freeze Information

In some US states, you have the right to place a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. You can obtain further information regarding security freezes from the FTC and from any of the three credit reporting agencies listed below.

Equifax	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(800) 916-8800
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 9532	P.O. Box 105281
Atlanta, GA 30374	Allen, TX 75013	Atlanta, GA 30348

Maryland Residents

Visit the Maryland Office of the Attorney General website at www.oag.state.md.us/idtheft/index.htm. Call 1-410-528-8662 or write to: Consumer Protection Division, Maryland Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202

North Carolina Residents

Visit the North Carolina Office of the Attorney General at http://www.ncdoj.gov/Crime.aspx Call 1-919-716-6400 or write to: Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001

California Residents

State law requires us to inform you that law enforcement did not ask us to delay notification to you.

IRS Tax Return Information

If you suspect that a fraudulent tax return has or may be filed using your social security number, you should contact the IRS and file a complaint immediately. For more information, see https://www.irs.gov/uac/taxpayer-guide-to-identity-theft. If you receive a letter from the IRS indicating that there has been fraudulent activity, see the information at https://idverify.irs.gov/IE/e-authenticate/welcome.do. The TurboTax website also has good information at https://turbotax.intuit.com/tax-tools/tax-tips/General-Tax-Tips/Identity-Theft--What-to-Do-if-Someone-Has-Already-Filed-Taxes-Using-Your-Social-Security-Number/INF23035.html.

The Official Website of the Office of Consumer Affairs & Business Regulation (OCABR)

Consumer Affairs and Business Regulation

Home > Data Privacy and Security > Data Breach > Security Breach Notifications Submission

Security Breach Notifications Submission

Instructions: Please complete the form below to submit a data breach notification to the Office of Consumer Affairs and Business Regulation. You can also print this submission for your own records. Please note under M.G.L. C93H, a separate notification must be sent to the Attorney General's Office. **Please do not include any personally identifiable information for Massachusetts residents in any of the fields.**

Section I: Organization & Contact Information

Business Name*
Outten & Golden LLP

Business Address*
3 Park Avenue
29th Floor
New York (City) | New York (State) | 10016 (ZIP Code)

Company Type*
Commercial

Your Name*
Jason (First Name) | Bernstein (Last Name)

Title*
Partner

Contact Address*
3475 Piedmont Road, NE
Suite 1700
Atlanta (City) | Georgia (State) | 30022-3327 (ZIP Code)

Telephone Number*
(404) 264-4040

Extension

Email Address*
jason.bernstein@btlaw.com

Relationship to Org*
Third party provider

Section II: Breach Information

Breach Type*
Electronic

Date Breach was Discovered*
06 18 2016

Number of Massachusetts Residents Affected*
1

Person responsible for data breach.*
Current Employee

Please give a detailed explanation of how the data breach occurred.*

Employee was a victim of a phishing attack and sent a file with the W2 information of the firm's employees to an unauthorized email address.

710/850

Please select the type of personal information that was included in the breached data.*

	Selection(s)
Financial Account Numbers	☐
Social Security Numbers	☑
Driver's License	☐
Credit/Debit Card Number	☐

Please check ALL of the boxes that apply to your breach.*

	Selection(s)
The person(s) with possession of personal information had authorized access	☐
The breach was a result of a malicious/criminal act.	☑
The breach occurred while the data was being transported outside of your premises.	☐
The breach occurred at the location of a third party service provider.	☐
There is a written contract in place with the third-party provider requiring protection of personal information.	☐

Section III: Security Environment

For breaches involving paper: A lock or security mechanism was used to physically protect the data.*

- ☐ Yes
- ☐ No
- ☑ N/A

Physical access to systems containing personal information was restricted to authorized personnel only.*

- ☐ Yes
- ☐ No
- ☑ N/A

Network configuration of breached system*

Internet Access Available ▾

For breaches involving electronic systems, complete the following*

	Selection(s)
Breached data was encrypted.	☐
The key to encrypted data was stolen.	☐
Personal information stored on the breached system was password-protected and/or restricted by user permissions.	☑
N/A	☐

Section IV: Remediation

All Massachusetts residents affected by the breach have been notified of the breach.*

☑ Yes
☐ No

Method(s) used to notify Massachusetts residents affected by the breach (check all that apply):*

	Selection(s)
E-mail	☑
US Mail	☐
Online posting	☐
TV/Radio publication	☐
Other	☐

Date notices were first sent to Massachusetts residents (MM/DD/YYYY)*

06 ▾ 19 ▾ 2016 ▾

All Massachusetts residents affected by the breach have offered complimentary credit monitoring services .*

☑ Yes
☐ No

Law enforcement has been notified of this data breach.*

☑ Yes
☐ No

Please describe how your company responded to the breach. Include what changes were made or may be made to prevent another similar breach from occurring.*

The company investigated the breach to determine the cause. Improved procedures were implemented for verifying/validating information requests (e.g., W-2 requests).

685/850

**Any documents pertaining to the data breach including the letter being sent to the Massachusetts residents must be sent via email to data.breaches@state.ma.us

Please do not include any personally identifiable information for Massachusetts residents in any email attachment.

Please review the information you have entered and click on the "Submit Form" button below.

Submit Form

Please print this page before submitting.

Print This Page

Did you find the information you were looking for on this page? *

○ Yes
○ No